

FILED

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA**

## Alexandria Division

2014 JUL 18 P 2:49

VERISIGN, INC.,

Plaintiff,

**V.**

TUCOWS.COM CO.,

Defendant.

CLERK US DISTRICT COURT  
ALEXANDRIA, VIRGINIA

Civil Action No. 1:14cv624 LMB / JFA

**Filed Under Seal**

REDACTED

**BRIEF IN OPPOSITION TO MOTION TO DISMISS**

The plaintiff, VeriSign, Inc. (“Verisign”), states the following as its brief in opposition to Defendant’s Motion to Dismiss (Dkt. 12).

## I. Introduction

This action involves a two-count claim by Verisign, in which Verisign seeks to recover its contractually-allowed fees for providing DDoS mitigation services for Tucows.com Co. (“Tucows”), at Tucows’ request. At bottom, this case is a payment dispute. About a week before Christmas last year, Tucows’ networks and its websites were subject to cyber-attacks by nefarious actors who tried to bring the websites off line and make them inaccessible to visitors by flooding the servers with garbage queries. This is called a DDoS attack. Because Tucows is one of Verisign’s DDoS protection services customers, Verisign was monitoring Tucows’ networks and Verisign detected the DDoS attacks. Verisign then alerted Tucows of the situation and asked whether Tucows wanted Verisign to try to stop the attacks – i.e., mitigate the attacks. Tucows confirmed that it did. Verisign then successfully defeated the attacks. Tucows’ websites did not go off line and it enjoyed the benefits of having its websites up and running during the busy holiday season.

The Agreement required Verisign to do all of this for free – except when the attack was large enough (i.e., a lot of garbage traffic) – which, in this instance it was. After the attack was defeated, however, Tucows decided it did not want to pay the fees associated with the attacks and has refused to do so for no good reason. This motion continues this pattern of seeking to avoid payment without any basis. Here, Tucows’ motion to dismiss challenges the existence of the contract itself. Below, Verisign will show how none of these challenges have merit.

## **II. Standard of Review**

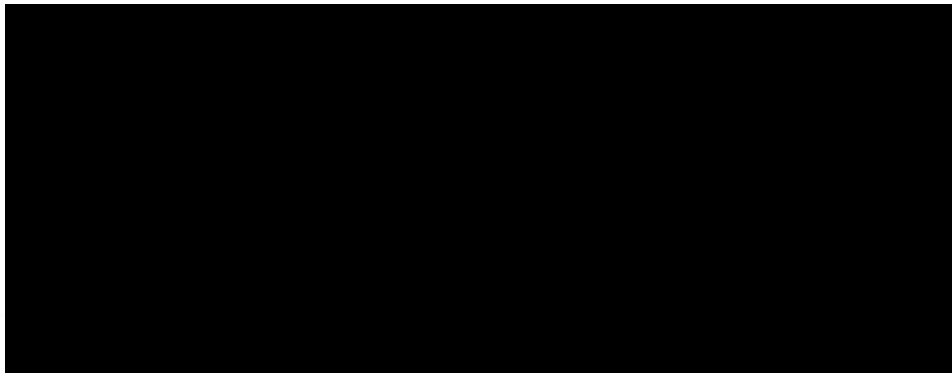
A complaint should not be dismissed, “unless it appears certain that plaintiff can provide no set of facts that would support his claim and would entitle him to relief.” *Brainware, Inc. v. Mahan*, 808 F. Supp. 2d 820, 825 (E.D. Va. 2001) (citing *Smith v. Sydnor*, 184 F.3d, 356, 361 (4th Cir. 1999)). The Court must accept all of the complaint’s well-pleaded allegations and view them in a light most favorable to the plaintiff. *Id.* “Factual allegations must be enough to raise a right of relief above the speculative level, on the assumption that all of the allegations in the complaint are true.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

## **III. Facts Alleged in the Complaint**

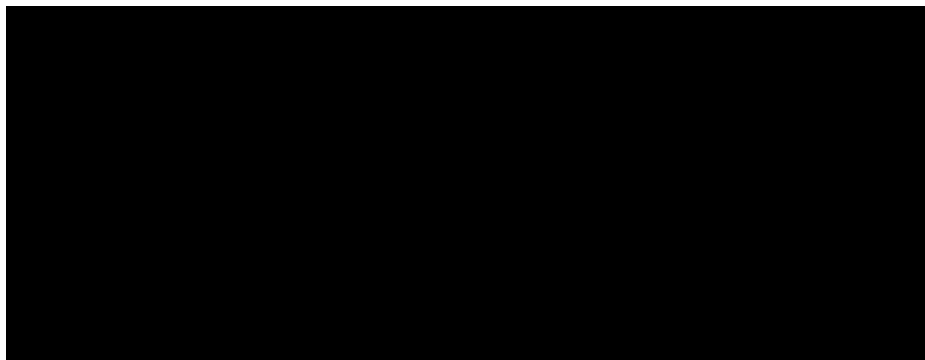
On November 16, 2009, Tucows and VeriSign entered into a VeriSign Internet Defense Network Evaluation Agreement (the “Agreement”), a copy of which is attached to the Complaint as *Exhibit 1*. (Compl. ¶ 8). The Agreement was for a term of 6 months, which automatically renewed for additional terms of 6 months each, until terminated by written notice. (Compl. ¶ 9). The Agreement was in full force and effect until March 2014. *Id.* Indeed, and Tucows’ protestations to the contrary notwithstanding, Tucows agreed that the Agreement remained in force until March 17, 2014, in a “Service Order Form for Verisign DDoS Protection Service” (the “SOF Contract”), a copy of which is attached hereto as *Exhibit A*. In the SOF Contract, Tucows concurred

that the SOF Contract was “to supersede and replace the Evaluation Agreement” and that as of March 17, 2014, “the Evaluation Agreement shall be (i) terminated and (ii) replaced and superseded by this” SOF Contract. *Ex. A*, at 1. Tucows understandably omits mention of this fact in its brief, as it is directly at odds with Tucows’ contention that the Agreement expired in 2010. Tucows seems to be arguing, now, that in 2014 it “superseded,” “replaced” and “terminated” a contract that – according to it – had not existed for more than 3 years.

Under the Agreement, Verisign was entitled to the payment of fees when it mitigated particularly large DDoS attacks at Tucows’ request. For instance, Section 2.3 of the Agreement provided, in pertinent part:



\* \* \*



(Compl. ¶ 11). Section 2.4 of the Agreement, in turn, provided that Verisign may invoice Tucows for additional fees incurred pursuant to Section 2.3 of the Agreement during the month following a Filtered DDoS Event, and that payment of such invoice would be due within 30 days of the invoice date. (Compl. ¶ 12).

On December 17, 2013, Verisign's DDoS monitoring service detected the occurrence of an initial DDoS attack on Tucows. (Compl. ¶ 13). Verisign contacted Tucows to alert it to the attack; Tucows confirmed it was experiencing a DDoS attack, and advised Verisign that it would let Verisign know if it desired that Verisign implement DDoS mitigation services (referred to in the Agreement as a "Filtered DDoS Event"). *Id.* Thereafter, Tucows requested that Verisign implement its DDoS mitigation services. (Compl. ¶ 14). This first Filtered DDoS Event then exceeded the thresholds provided in Section 2.3. (Compl. ¶¶ 15-17). On December 18, 2013, Lucian Floria, a member of Tucows' senior management, acknowledged that Tucows was liable for additional charges under the Agreement as a result of the DDoS attack that began on December 17, 2013. (Compl. ¶ 18). *See* Email dated December 18, 2013, from Lucian Florea to Michael Chase (of Verisign), a copy of which is attached hereto as *Exhibit B* ("I would suggest to treat this particular incident separately, as per our current contract and have the proposed discussion [regarding a new contract with different terms] in early January") (underscoring added).

On December 19, 2013, a second wave of DDoS attacks began on Tucows' network. (Compl. ¶ 19). That same day, Tucows again requested that Verisign implement its DDoS mitigation services with respect to the new attack. (Compl. ¶ 20). This second Filtered DDoS Event, like the first, then exceeded the thresholds provided in Section 2.3. (Compl. ¶¶ 21-23). Taha Hasan, a Tucows employee, acknowledged that Tucows was liable for additional charges under the Agreement as a result of the DDoS attack that began on December 19, 2013. (Compl. ¶ 24). Verisign ultimately treated the two attacks as a single Filtered DDoS Event, to reduce the charges payable by Tucows. (Compl. ¶ 25).

Verisign then issued an invoice for \$320,000.00 to Tucows on January 13, 2014 (the "Invoice"). (Compl. ¶ 27). Tucows has refused to pay the Invoice. (Compl. ¶¶ 28-29).

#### IV. Argument

##### A. Count I of the Complaint States a Plausible Claim for Breach of Contract.

##### 1. The Agreement did not expire until March 2014.

Tucows first argues that the Agreement expired by its own terms in 2010. In support of this contention, Tucows ignores the allegations in the Complaint; quotes a portion, but not all, of the Agreement;<sup>1</sup> and manufactures facts which are unsupported by the allegations in the Complaint. Tucows further entirely ignores the fact that it took the position, up until the time it filed its Motion to Dismiss, that the Agreement was valid and subsisting until March 2014, when it entered into another agreement with Verisign which, by its terms, replaced and terminated the Agreement.

The term of the Agreement is defined in Section 5.1:

Unless earlier terminated as set forth herein, the term of this Agreement shall commence upon the Effective Date [November 16, 2009] and shall continue for six (6) months from the Activation Date (the "Initial Term"). Upon expiration of the Initial Term, this Agreement shall automatically renew for an additional six (6) months (each a "Renewal Term" and, together with the Initial Term, the "Term") . . . .

Tucows contends that this language provides for a single six-month Renewal Term, citing to the use of the singular word "an."

However, "contracts must be considered as a whole 'without giving emphasis to isolated terms.'" *TM Delmarva Power, LLC v. NCP of Va., LLC*, 263 Va. 116, 119, 557 S.E.2d 199, 200

---

<sup>1</sup> Tucows also mischaracterizes other portions of the Agreement. For instance, it states "that the terms of the Agreement may only be modified 'by an instrument in writing duly agreed to and executed by the parties.'" Tucows Brief at 7, n.8 (citing Section 12.1 of the Agreement). In fact, Section 12.1 of the Agreement does not provide that written modification is the only means of modifying the Agreement. It states only the truism that "The parties may modify any of the provisions of this Agreement by an instrument in writing duly agreed and executed by both parties."

(2002) (quoting *American Spirit Ins. Co. v. Owens*, 261 Va. 270, 275, 541 S.E.2d 553, 555 (2001)). Further, “no word or clause in the contract will be treated as meaningless if a reasonable meaning can be given to it, and there is a presumption that the parties have not used words needlessly.” *Preferred Sys. Solutions, Inc. v. GP Consulting, LLC*, 284 Va. 382, 392, 732 S.E.2d 676, 681 (2012); *Dragas Mgt. Corp. v. Hanover Ins. Co.*, 798 F. Supp. 2d 766, 772 (E.D. Va. 2011).<sup>2</sup> Yet Tucows asks the court to ignore the phrase “each a ‘Renewal Term,’” which connotes that there may, in fact, be more than one renewal period. If not, the word “each” is mere surplusage and must be read as meaningless. The word “an” is not, as Tucows argues, an antecedent to “renewal term.” It modifies “six (6) months.” Thus, the clear intent of this clause was to provide for an initial term of six months, and a series of renewal terms, each of which was six months in length. While not a model of clear drafting, the intent of the parties is clear from a reading of the entirety of Section 5.1.<sup>3</sup> In sum, the Agreement automatically renewed in six-month increments. Verisign alleged in the Complaint (¶ 9) that the Agreement was in fact renewed until terminated in March 2014, after the events which gave rise to this action. Tucows’ argument to the contrary must be rejected.

---

<sup>2</sup> Virginia law applies to the interpretation of the Agreement, per Section 12.3 of the Agreement. See also *Seabulk Offshore Ltd. v. Amer. Home Assurance Co.*, 377 F.3d 408, 418-19 (4th Cir. 2012) (discussing choice of law rules applicable to contract interpretation in a diversity action).

<sup>3</sup> Tucows argues that to the extent Section 5.1 is ambiguous, it must be construed against the drafter. Tucows so argues without any reference to an allegation in the Complaint to the effect that Verisign was the sole drafter, nor does it provide any evidence establishing that Verisign was the sole drafter of the Agreement. Yet it makes such statements as “Verisign openly admits that it drafted the Agreement,” Tucows Brief at 7, then cites to allegations in the Complaint that do not support this proposition in any way. If the Agreement is ambiguous, then parol evidence is necessary to explain its meaning. See, e.g., *Murr v. Capital One Bank (USA), N.A.*, 2014 WL 2933242, \*7-8 (E.D. Va., June 27, 2014) (denying summary judgment in light of ambiguous contractual provision). Tucows’ motion to dismiss must, for that reason alone, be denied.

In any event, where, as here, the parties treat a contract as ongoing, the law treats the contract as in fact ongoing, in accordance with the parties' own actions:

general principles of contract law teach us that when a contract lapses but the parties to the contract continue to act as if they are performing under a contract, the material terms of the prior contract will survive intact unless either one of the parties clearly and manifestly indicates, through words or through conduct, that it no longer wishes to continue to be bound thereby, or both parties mutually intend that the terms not survive. The rationale for this rule is straightforward: when parties to an ongoing, voluntary, contractual relationship, especially a relationship which by its nature generally implies that *some* mutually agreed upon rules govern its contract configuration, continue to behave as before upon the lapse of the contract, barring contrary indications, each party may generally reasonably expect that the lapsed agreement's terms remain the ones by which the other party will abide.

*Luden's, Inc. v. Local Union No. 6*, 28 F.3d 347, 355-56 (3d Cir. 1994) (italics in original). *See also, Riso, Inc. v. Witt Co.*, 2014 WL 3371731, \*19 (D. Or., July 9, 2014) ("as a general rule, an implied agreement arises when a written contract expires by its terms and the parties continue to perform as before"); *Andrews v. Sotheby Int'l Realty, Inc.*, 2014 WL 626968, \*8 (S.D.N.Y., Feb. 18, 2014) (where parties' conduct after expiration of a written contract is in accordance with the terms of the written contract, this establishes a "contract implied in fact with substantially the same terms and conditions as embodied in the expired written contract") (internal quotation marks omitted); *Darling Int'l, Inc. v. Baywood Partners, Inc.*, 2006 WL 2374635, \*5 (N.D. Cal., Aug.

16, 2006) (subsequent conduct of the parties may be considered as evidence of the parties' understanding that the contract did or did not terminate on its own accord").<sup>4</sup>

However, a parsing of the exact language used in the Agreement is in point of fact unnecessary here, because the parties in any event treated the Agreement as valid, binding and subsisting until March 2014. As noted in the Complaint and above, in December 2013, Tucows representatives recognized and acknowledged that the Agreement remained in place. *See* Complaint ¶¶ 18, 24; *Ex. B*, attached hereto.<sup>5</sup> And in March 2014, Tucows entered into another contract with Verisign which, by its terms, terminated, replaced and superseded the Agreement.

So even accepting, *arguendo*, Tucows' argument that the term of the Agreement was limited to a single six-month renewal term, the fact that the parties treated the Agreement as effective up until March 2014 establishes that the parties did in fact have a contract, on the terms set forth in the Agreement, until that time. Therefore, Tucows' argument that the Agreement was terminated no later than November 2010 is unsupported by conduct, including execution of the SOF Contract, and unsupported by the plain meaning of the Agreement itself.

---

<sup>4</sup> Virginia has adopted this rule, in a slightly different context. *See Miller v. SEVAMP, Inc.*, 234 Va. 462, 465, 362 S.E.2d 915, 916 (1987) ("If an employee enters the employment of another for a definite period (one year or less) and continues in that employment after the expiration of the agreed period, without any new agreement, a rebuttable presumption arises that the contract has been renewed for a like term."). Many other courts have likewise recognized this principle. *See, e.g., Cloverdale Equip. Co. v. Manitowoc Eng. Co.*, 964 F. Supp. 1152, 1162 (E.D. Mich. 1997) (where parties continued doing business as usual following the expiration of the written agreement, "an implied in fact agreement was created, which incorporated the same material terms"); *Nat'l Union Fire Ins. Co. v. Showa Shipping Co., Ltd.*, 166 F.3d 343, \*3, n.6 (9th Cir. 1999) (same); *Jurrens v. Lorenz Mfg. Co.*, 578 N.W.2d 151, 153 (S.D. 1998) (quoting *Martin v. Campanaro*, 156 F.2d 127, 129 (2d Cir.), *cert. denied*, 329 U.S. 759 (1946)) ("When an agreement expires by its terms, if, without more, the parties continue to perform as theretofore, an implication arises that they have mutually assented to a new contract containing the same provisions as the old").

<sup>5</sup> In addition, while unnecessary here, Verisign will also present evidence if needed that it performed other DDoS mitigation services for Tucows, at Tucows' request, during the period between 2010 and 2014. In all such cases, the parties treated these services as being performed under the Agreement.



## 2. The Agreement is not affected by the doctrine of mutuality.

Tucows next argues that the Agreement is void because of a purported lack of mutuality. To support this argument, Tucows invents provisions of the Agreement which simply do not exist, to support its argument that Verisign had no obligation to perform under the Agreement. Moreover, Tucows applies a shallow analysis of the law governing mutuality, painting an inaccurate portrait of the showing it must make to support its arguments.

The doctrine of mutuality provides that “when two parties have exchanged promises as consideration, each must be bound to do or refrain from doing something.” *Bartley v. Merrifield Town Center Ltd. P’Ship*, 580 F. Supp. 2d 495, 502 (E.D. Va. 2008) (citing *C.G. Blake Co. v. W.R. Smith & Son*, 147 Va. 960, 133 S.E. 685, 688 (1926)). “Thus, ‘[i]f it appears that one party was never bound on its part to do the acts which form the consideration for the promise of the other, there is a lack of mutuality of obligation and the other party is not bound.’” *Id.*, quoting *Busman v. Beeren & Barry Invs., LLC*, 69 Va. Cir. 375 (2005). However, a “discrepancy in available remedies between the two parties does not amount to a lack of mutuality.” *Bartley*, 580 F. Supp. 2d at 503. Moreover, a clause allowing a party to terminate a contract upon some notice to the other does not result in a lack of mutuality. *See Gay Nineties, Inc. v. Int’l Dining Club*, 21 Va. Cir. 492 (1973) (holding that a clause allowing a party to terminate on 30 days’ notice did not destroy mutuality).

Further, “mutuality of promises provides consideration by each party, even if the promises relate to different terms of the contract or depend on the performance of the other party.” *Suntrust Mortg., Inc. v. Security First Bank*, 2012 WL 777933, \*2 (E.D. Va., Mar. 7, 2012) (citing *C.G. Blake Co. v. W.R. Smith & Son, Ltd.*, 147 Va. 960, 971–72, 133 S.E. 685 (1926)). “In sum, for a

contract to be enforceable, both parties must be bound to the agreement by the exchange of promises to act or refrain from acting.” *Id.*

In addition, and ignored by Tucows, “[m]utuality is determined not at the time of the creation of the contract, but at the time the contract is sought to be enforced.” *Security First*, 2012 WL 777933, at \*3 (citing *Asberry v. Mitchell*, 121 Va. 276, 281, 93 S.E. 638 (1917)) (testing mutuality at the institution of the suit). “Thus, a contract that lacks mutuality at its creation may still be enforceable if the parties act in a manner, post-contract creation, that indicates their intent to be bound by the contract.” *Id.* (citing *Schwam v. XO Commc’ns, Inc.*, 2006 WL 6884392, \*9 (4th Cir., Mar. 24, 2006)). Therefore, if the parties, by their actions, treat the agreement as an enforceable one, such “actions erase[] any defect that may have existed at formation, and the result is an enforceable contract.” *Suntrust Mortg., Inc. v. Simmons*, 861 F. Supp. 2d 733, 736 (E.D. Va. 2012).

As an initial matter, as alleged in the Complaint, the parties at all times treated the Agreement as enforceable, with Verisign performing DDoS mitigation services, at Tucows’ request and with Tucows’ acknowledgement that Verisign was doing so under the Agreement, in December 2013. *See* Complaint ¶¶ 14, 18, 20, 24. Thus, the parties, by their actions, unequivocally treated the Agreement as enforceable and as if they intended to be bound, regardless of any mutuality issues. *See Schwam*, 2006 WL 6884392, at \*9; *Simmons*, 861 F. Supp. 2d at 736. *See* also, *Walter E. Heller & Co., Inc. v. Convalescent Home of the First Church of Deliverance*, 49 Ill. App. 3d 213, 220, 365 N.E.2d 1285, 1290 (1977) (citing 1A *Corbin on Contracts*, § 142, at 4-6 (1963)) (“Want of mutuality is no defense where a contract is executed or where a party who was not bound to perform does perform”). Therefore, the Court need not even consider Tucows’ various arguments regarding contractual language that it contends adversely affects mutuality, as

there is no dispute here – at least at this stage of the proceedings – that Verisign did in fact perform under the Agreement.

But even if the Court considers the various provisions that Tucows contends impair mutuality, the inescapable conclusion must be that Tucows' arguments are unmeritorious. Each of the provisions cited by Tucows will be addressed *seriatim* below.

A. *Calling the Agreement an "Evaluation Agreement" is irrelevant to mutuality.*

Tucows first argues that the Agreement lacks mutuality because it is called an "Evaluation Agreement" and because one of the "WHEREAS" clauses of the Agreement provides that Verisign will provide its Internet Defense Network Service and that Tucows "desires to use [such service] on an evaluation basis." Tucows Brief at 8. Tucows never explains how this has any effect whatsoever on the parties' mutual obligations, nor is the meaning of this argument apparent. At bottom, Section 2.1 of the Agreement provides for the parties' mutual exchange of consideration:

2.1 Consideration. During the Term and subject to Sections 1.2.3.4, 2.2 and 2.3 [which provides for the fees sued for here], Verisign will provide the VeriSign Internet Defense Network Service in exchange for the following: (i) Feedback provided by Customer in accordance with Section 5.1 herein; and (ii) Customer will serve as a reference account for the VeriSign Internet Defense Network Service in support of VeriSign's sales efforts. For avoidance of doubt, except as set forth below and in Section 1.2.3.4, VeriSign will not charge Customer its standard fees for the VeriSign Internet Defense Network Service.

The use of the word "evaluation" in the Agreement is wholly irrelevant to a consideration of whether there was mutuality of obligation.

B. *Section 3.1 of the Agreement does not allow Verisign to unilaterally elect not to perform.*

Tucows next argues that Section 3.1 of the Agreement demonstrates a lack of mutuality because, Tucows states, it allows "Verisign to unilaterally elect not to perform any DDoS

mitigation service and will [sic] only notify Tucows of this election not to perform ‘if reasonably practicable to do so.’” Tucows Brief at 8. In fact, Section 3.1 does not so state. It provides:

3.1 If the bandwidth of a DDoS Event is greater than the shared capacity of the VeriSign Internet Defense Service, or if the event is impacting the operational stability of VeriSign, VeriSign may choose (i) not to accept all or a part of Customer’s Internet Traffic; or (ii) drop all or part of Customer’s Internet Traffic from the VeriSign Internet Defense Network sites; *provided, however*, that VeriSign will notify Customer in advance if it is reasonably practicable to do so.

Section 3.1 of the Agreement, therefore, provides for two enumerated situations in which Verisign may elect to limit provision of its services, and provides that Verisign will give notice of such action in advance when practicable. Verisign is bound to perform, unless the specified conditions are met. This does not affect mutuality in the least. This provision does not, as Tucows claims, allow Verisign to unilaterally elect not to perform. Tucows’ suggestion otherwise is entirely baseless.

C. *Section 4.2 of the Agreement does not allow Verisign to unilaterally adjust minimum thresholds.*

Tucows next argues that Section 4.2 of the Agreement demonstrates a lack of mutuality because, Tucows states, it allows “Verisign to unilaterally ‘adjust minimum thresholds’ on an as-needed basis.” Tucows Brief at 8-9. Again, through selective quotation, Tucows mischaracterizes what the Agreement in fact states. Section 4.2 provides:

4.2 Customer will cooperate with VeriSign to (i) determine initial minimum thresholds for Customer’s internet traffic; and (ii) adjust minimum thresholds during the term on an as needed basis.

This provision does not, as Tucows contends, allow Verisign to do anything “unilaterally.” It simply provides a covenant requiring Tucows to cooperate to set the initial thresholds (which was

actually done – *See* Agreement § 2.3) and to adjust them from time if needed. It does not allow Verisign to do anything “unilaterally” and has no effect whatsoever on mutuality.

D. *Section 5.2 of the Agreement, which allows each party to terminate the Agreement on 60 days’ notice, does not affect mutuality.*

Tucows next argues, without analysis, that Section 5.2 of the Agreement demonstrates a lack of mutuality because it allows each party to terminate the Agreement on 60 days’ notice to the other. Section 5.2 provides:

5.2 Termination for Convenience. Either party may terminate this Agreement for convenience upon providing the other Party with sixty (60) days prior written notice.

Such a provision, allowing a party to terminate a contract upon some notice to the other, does not result in a lack of mutuality. *See Gay Nineties, Inc. v. Int’l Dining Club*, 21 Va. Cir. 492 (1973).

E. *Section 5.4 of the Agreement does not allow Verisign to unilaterally terminate the agreement.*

Tucows next argues that Section 5.4 of the Agreement demonstrates a lack of mutuality because, Tucows states, it reserves “the right to Verisign alone to terminate the Agreement immediately ‘in its sole discretion.’” Tucows Brief at 9. Once again, through selective quotation, Tucows mischaracterizes what the Agreement actually states. Section 5.4 provides:

5.4 VeriSign’s Additional Termination Rights. Notwithstanding anything in this Agreement to the contrary and in addition to VeriSign’s rights under Sections 5.2 and 5.3 herein, VeriSign may terminate this Agreement immediately upon notice to Customer (i) in the event that VeriSign determines, in its sole discretion, that Customer has breached Section 3.2 herein [providing that Tucows represents that it is not engaged in illegal activities]; and (ii) in the event VeriSign determines, in its sole discretion, that it cannot increase the credit limit or grant net payment terms to Customer at any time during the Term.

This provision does not, as Tucows contends, allow Verisign to simply terminate the Agreement as a matter of discretion. It allows Verisign to terminate the Agreement only in two limited,

enumerated instances – if Verisign determines that Tucows is engaged in illegal activity, or if Verisign determines that Tucows creditworthiness is impaired. This is a far cry from Tucows’ characterization of Section 5.4 as permitting Verisign to simply terminate the Agreement at its discretion at any time.

F. *Section 10 of the Agreement – which contains a disclaimer of warranties – does not impair mutuality of contract.*

Tucows next argues, again without analysis, that Section 10 of the Agreement demonstrates a lack of mutuality because in that section, Verisign disclaims certain warranties. Tucows Brief at

9. Section 10 provides:

10. DISCLAIMER. THE VERISIGN INTERNET DEFENSE NETWORK SERVICE IS PROVIDED “AS IS”, “AS AVAILABLE” AND WITHOUT ANY WARRANTY [sic] WHATSOEVER. VERISIGN DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY ARISING OUT OF A COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. VERISIGN DOES NOT REPRESENT, WARRANT OR GUARANTEE THAT THE VERISIGN INTERNET DEFENSE NETWORK SERVICE PROVIDED HEREUNDER WILL BE UNINTERRUPTED, UNDISRUPTED OR ERROR-FREE.

Tucows cites to no authority suggesting that a disclaimer of warranties impairs mutuality. And to Verisign’s knowledge, there is none. This is so because a disclaimer of warranties has nothing to do with the parties’ fundamental exchange of promises. Here, in the Agreement, Verisign agreed to perform services to Tucows, if Tucows so requested, and Tucows agreed to provide feedback and references, and to pay for those services once a certain threshold was exceeded. Limitations as to the scope or adequacy of those services are irrelevant to the inquiry as to whether the parties are each bound to do something. Therefore, a disclaimer of warranties does not impair mutuality.

G. *Section 11 of the Agreement – which contains limitations on the liabilities of the parties – does not impair mutuality of contract.*

Tucows next argues, yet again without analysis, that Section 11 of the Agreement establishes a lack of mutuality because, Tucows claims, it disclaim[s] all liability. Tucows Brief at 9. It does not. Section 11 provides:

11. LIMITATION OF LIABILITY. (A) EXCEPT AS SET FORTH IN PARAGRAPH (C) BELOW, VERISIGN'S ENTIRE LIABILITY AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM ARISING OUT OF THIS AGREEMENT IS LIMITED TO THE AMOUNTS PAID OR PAYABLE BY CUSTOMER TO VERISIGN FOR THE VERISIGN INTERNET DEFENSE NETWORK SERVICE PROVIDED HEREUNDER [sic]. (B) NEITHER PARTY SHALL BE LIABLE FOR ANY CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR REVENUES, WHETHER FORSEEABLE OR UNFORSEEABLE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ARISING OUT OF THIS AGREEMENT, THE SERVICES, FOTWARE, OR HARDWARE OR ANY EXPRESS OR IMPLIED WARRANTY, MISREPRESENTATON, NEGLIGENCE, STRICT LIABILITY OR OTHER TORT. (C) VERISIGN SHALL HAVE NO LIABILITY (i) TO THE EXTENT THAT CUSTOMER DELAYS IN REDIRECTING ITS INTERNET TRAFFIC OR IN THE EVENT THAT CUSTOMER DOES NOT REDIRECT ITS INTERNET TRAFFIC OR DISCONTINUES REDIRECTING ITS INTERNET TRAFFIC DURING A FILTERED DDOS EVENT; AND (ii) WITH RESPECT TO THE AUP OR ANY ACTION TAKEN, OR INACTION, BY VERISIGN IN CONNECTION WITH THE AUP (INCLUDING, BUT NOT LIMITED TO, IN RELATION TO ANY VIOLATION OF THE AUP).

Tucows cites no authority suggesting that a limitation of remedies clause impairs mutuality, and with good reason – Section 11 does not provide that Tucows has no remedies in the event of a breach of the Agreement by Verisign. Tucows' citation to Section 11 to support its position is puzzling. Since Section 11 allows Tucows some remedy in the event of a breach of the Agreement by Verisign, it has no effect on mutuality. *See, e.g., Fransmart, LLC v. Freshii Dev., LLC*, 768 F.

Supp. 2d 851, 870 (E.D. Va. 2011) (“Freshii argues that Fransmart has not bound itself to perform because it suffers no penalty by simply choosing not to market and sell Freshii’s franchises. This argument is unpersuasive because, although the Agreement provides that Freshii *may* terminate the Agreement if Fransmart fails to meet its sales quota or is otherwise in material breach, there is nothing in the Agreement stating that Freshii’s *sole* remedy is termination.”).

H. *Section 5 of the Acceptable Use Policy does not allow Verisign to unilaterally terminate the agreement.*

Tucows lastly argues Section 5 of the Acceptable Use Policy (“AUP”) attached to the Agreement demonstrates a lack of mutuality because, Tucows states, it allows “Verisign to terminate the Agreement at any time in its sole discretion.” Tucows Brief at 9. Yet again, through selective quotation, Tucows mischaracterizes what the AUP actually states. Section 5 of the AUP provides:

5. VeriSign’s Rights. If VeriSign determines, in its sole discretion, that Customer has failed to comply with any provision of the AUP, or undertakes or attempts to undertake any of the prohibited activities described herein, Customer agrees that VeriSign may immediately take corrective action which includes, but is not limited to, suspension of the VeriSign Internet Defense Network Service and/or termination of this Agreement. Such corrective action is in addition to any other rights of VeriSign under the Agreement, this AUP or under law. VeriSign may provide Customer with notice that VeriSign intends to take action under this Section 5 but is not required to do so.

This provision does not, as Tucows contends, allow Verisign to simply terminate the Agreement. It allows Verisign to suspend or terminate the Agreement in the event Tucows violates the AUP. Tucows’ characterization of this provision is, as with its other characterizations of provisions of the Agreement, far afield from the accurate, fair statements one would expect. The provision of remedies – including termination – as a result of a party’s breach of an agreement is irrelevant to a determination of the existence or non-existence of mutuality.



### 3. The Agreement is not an unenforceable “agreement to agree.”

Tucows next argues that the Agreement is a mere “agreement to agree” and, therefore is unenforceable. It does so by completely misstating the holdings in applicable case law, then mischaracterizing provisions in the Agreement.

As to the authorities cited by Tucows, in *Kay v. Prof'l Realty Corp.*, 222 Va. 348, 281 S.E.2d 820 (1981) and *Allen v. Aetna Cas. & Sur. Co.*, 222 Va. 361, 281 S.E.2d 818 (1981), the Court held only that an “agreement ‘to negotiate a settlement’ constituted nothing more than an agreement to agree upon a settlement at a later date;” and that an “agreement to negotiate fails to provide a reasonably certain basis for determining an adequate remedy and therefore is unenforceable.” *Kay*, 222 Va. at 351, 281 S.E.2d at 822; *see Allen*, 222 Va. at 364, 281 S.E.2d at 820. Tucows also cites to *Beazer Homes Corp. v. VMIF/Anden Southbridge Venture*, 235 F. Supp. 2d 485 (E.D. Va. 2002) for the same proposition, despite its holding which is substantively identical to that in *Kay* and *Allen*. Yet the Agreement provides very precise remedies for both parties – Verisign is entitled to payment for its services in accordance with a detailed formula. Agreement § 2.3. And Tucows is entitled to recover from Verisign, in the event Verisign breaches the Agreement, Tucows may in general recover money damages up to the amounts paid or payable by it. Agreement § 11.

Tucows then proceeds to mischaracterize provisions in the Agreement. First, it contends that Section 3.1 of the Agreement “allows Verisign to unilaterally elect not to perform any DDoS mitigation service, or if [it] did elect to perform it could decide to what extent it performed,” and that Verisign “was not even required to inform Tucows of its election to ignore the Agreement.” Tucows Brief at 10. Tellingly, Tucows does not recite the actual words used in Section 3.1 of the Agreement, which reveal that its characterization thereof is grossly inaccurate:

3.1 If the bandwidth of a DDoS Event is greater than the shared capacity of the VeriSign Internet Defense Service, or if the event is impacting the operational stability of VeriSign, VeriSign may choose (i) not to accept all or a part of Customer's Internet Traffic; or (ii) drop all or part of Customer's Internet Traffic from the VeriSign Internet Defense Network sites; *provided, however*, that VeriSign will notify Customer in advance if it is reasonably practicable to do so.

Section 3.1 of the Agreement, therefore, provides for two enumerated situations in which Verisign may elect to limit provision of its services, and provides that Verisign will give notice of such action in advance when practicable. This is a sort of very limited *force majeure* clause, which most assuredly does not, as Tucows claims, allow Verisign to unilaterally decide elect whether to perform, and does not allow Verisign to ignore the Agreement.

Second, Tucows continues with its mischaracterization of the Agreement, contending that Section 4.2 "allows Verisign to unilaterally 'adjust minimum thresholds' of the relevant internet traffic on an 'as needed basis.'" Once again, Tucows declines to quote all of the language of the provision, as the actual words used in the Agreement demonstrate that Tucows is fabricating a meaning and intent that are not present in the Agreement. Section 4.2 provides:

4.2 Customer will cooperate with VeriSign to (i) determine initial minimum thresholds for Customer's internet traffic; and (ii) adjust minimum thresholds during the term on an as needed basis.

This provision does not, as Tucows contends, allow Verisign to do anything "unilaterally." It simply provides a covenant requiring Tucows to cooperate to set the initial thresholds (which was actually done – *See* Agreement § 2.3) and to adjust them from time to time if necessary.

Simply put, the Agreement is not, as Tucows suggests, an unenforceable agreement to reach an agreement in the future. Verisign and Tucows reached a clear contract – that Verisign would, within stated limits, provide DDoS mitigation services; and that when the amount of filtered traffic exceeded certain enumerated thresholds, and when Tucows requested Verisign to

perform the filtering, Tucows would pay Verisign fees in accordance with a specified formula. This is no “agreement to agree.” It is an agreement that Tucows agreed to, concurred with, and operated under, until it came time to pay.

**B. Count II of the Complaint States a Plausible Alternative Claim for Quantum Meruit.**

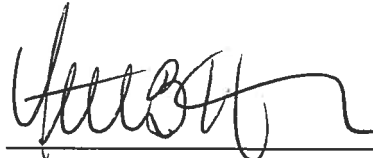
Tucows lastly argues that Count II of the Complaint – which states a cause of action for *quantum meruit* – must be dismissed if Verisign’s breach of contract claim contained in Count I survives. In support of this argument, Tucows cites to cases holding that recovery under a quasi-contractual claim is barred where there exists an express contract covering the same subject matter. *See, e.g., Mongold v. Woods*, 278 Va. 196, 204, 677 S.E.2d 288, 292 (2009). Tucows neglects to address the fact that Verisign’s *quantum meruit* claim is expressly brought as an alternative claim to its breach of contract claim. *See* Compl. at p.6, heading (“Count II (Quantum Meruit – Alternative to Count I”). Verisign’s caution in bringing this alternative claim has proven judicious by Tucows’ disavowal of the Agreement – wrongheaded as it is – in its motion to dismiss.

The law is clear that a plaintiff is permitted to plead claims under an express contract and a *quantum meruit* claim in the alternative, just as Verisign did here. *See Harrell v. Colonial Holdings, Inc.*, 923 F. Supp. 2d 813, 826-27 (E.D. Va. 2013) (denying motion to dismiss quasi-contractual claim brought in the alternative because while “Defendants cannot recover for breach of contract and unjust enrichment, they are allowed to plead these inconsistent theories”); *Kelly v. Ammodo Internet Svcs. Ltd.*, 2012 WL 4829341, \*5 (E.D. Va., Oct. 10, 2012) (same); *Mendoza v. Cedarquist*, 2009 WL 1254669, \*3 (E.D. Va., May 6, 2009) (Brinkema, J.) (“under Virginia and federal law, a plaintiff is permitted to plead equitable theories of relief such as unjust enrichment and *quantum meruit* as alternatives to contract recovery” and it is “eminently reasonable” to do so where the defendant is taking issue with the existence of the express contract); *Ford v. Torres*,

2009 WL 537563, \*4 (E.D. Va., Mar. 3, 2009). Tucows' suggestion that Count II of the Complaint must be dismissed if Count I survives is simply incorrect as a matter of well-established law. Verisign is entitled to bring alternative claims, and did so here. While Verisign cannot ultimately recover under a *quantum meruit* theory if there is a valid and subsisting contract covering the identical subject and time, it certainly may, and did, allege the claims in the alternative. Tucows' motion to dismiss Count II must therefore be denied.<sup>6</sup>

**V. Conclusion**

In its Motion to Dismiss, Tucows repeatedly ignores the facts alleged in the Complaint, mischaracterizes and misstates the terms of the Agreement, misapplies case law, and ignores many applicable concepts of law. Its Motion to Dismiss should summarily be denied.




---

Timothy B. Hyland  
 Virginia Bar No. 31163  
 Counsel for VeriSign, Inc.  
 HYLAND LAW PLLC  
 1818 Library Street, Suite 500  
 Reston, VA 20190  
 Tel.: (703) 956-3566  
 Fax: (703) 935-0349  
 Email: thyland@hylandpllc.com

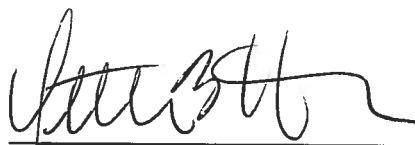
---

<sup>6</sup> Aside from its contention that Count I and Count II cannot survive in tandem, Tucows does not suggest that Verisign has not stated facts necessary to establish the existence of a claim for *quantum meruit*.

**CERTIFICATE OF SERVICE**

I HEREBY CERTIFY that a true copy of the foregoing was sent by email and mailed, first class mail, postage prepaid, this 18th day of July, 2014, to:

Sean Patrick Roche, Esquire  
CAMERON/MCEVOY, PLLC  
11325 Random Hills Road, Suite 200  
Fairfax, Virginia 22030

A handwritten signature in black ink, appearing to read 'Timothy B. Hyland', written over a horizontal line.

Timothy B. Hyland  
Virginia Bar No. 31163  
Counsel for VeriSign, Inc.  
HYLAND LAW PLLC  
1818 Library Street, Suite 500  
Reston, VA 20190  
Tel.: (703) 956-3566  
Fax: (703) 935-0349  
Email: thyland@hylandpllc.com

# EXHIBIT A



# Service Order Form for Verisign DDoS Protection Service

Customer: Tucows.com Co.  
Address: 96 Mowat Ave., Toronto ON M6K 3M1  
Canada

Primary Contact: Lucian Florea  
Telephone: 416-535-0123 ext 1282  
Email: lflorea@tucows.com

Accounts Payable/Billing Contact:  
Address:  
Telephone:  
Email:  
Reference number (if required):

## FOR VERISIGN INTERNAL USE ONLY

SERVICE ORDER FORM NUMBER: 122014-030214

MSA CONTRACT NUMBER: 9162010-000707

MSA EFFECTIVE DATE: 3/17/2014

SERVICE DESCRIPTION NUMBER: VERSION 1.5  
(AS MODIFIED - 6.25.2013)

SERVICE ORDER FORM EFFECTIVE DATE: 3/17/2014

WHEREAS, VeriSign, Inc. ("Verisign") and Customer entered into that certain Verisign Internet Defense Network Evaluation Agreement dated November 16, 2009 (the "Evaluation Agreement"; and

WHEREAS, Verisign and Customer wish to enter into a new Service Order Form (this "Service Order Form") to supersede and replace the Evaluation Agreement;

NOW, THEREFORE, in consideration of the mutual covenants and premises contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Verisign and Customer hereby agree as follows:

This Service Order Form is entered into as of the Service Order Form Effective Date by and between VeriSign, Inc. ("Verisign") and Customer, and is hereby incorporated into the Verisign Master Services Agreement bearing the MSA Contract Number and/or MSA Effective Date identified above (the "MSA"). As of the Service Order Form Effective Date, the Evaluation Agreement shall be (i) terminated and (ii) replaced and superseded by this Service Order Form; provided, however, that the payment terms and obligations of Customer to Verisign under the Evaluation Agreement for services performed thereunder prior to the Service Order Form Effective Date of this Service Order Form shall survive. Under this Service Order Form, Customer hereby orders the Verisign DDoS Protection Service for the fees set forth in Table 1 below, and agrees to the Terms and Conditions set forth herein and in the Service Description(s) attached hereto as Exhibit A and incorporated herein by this reference (the "Terms and Conditions", the "Service Description" and, together with this Service Order Form and the MSA, the "Agreement").

Customer acknowledges that it has read the Terms and Conditions and the Service Description bearing the version number identified above and agrees to be bound by the terms and conditions contained therein. Capitalized terms used herein and not otherwise defined shall have the meanings set forth in the Terms and Conditions or the Service Description.



**TABLE 1 – VERISIGN DDOS PROTECTION SERVICE**  
**INITIAL TERM: 1 MONTH FROM MARCH 17, 2014**


Verisign DDOS Protection Fees				
SKU & Description	Non-Recurring Fee (Customer Set-up)	Recurring Fee		
26969	\$0	\$10,500		
Total Contract Value		\$10,500		
Monitoring				
# of Routers Monitored	# Monitored Entities			
N/A	N/A			
Mitigation				
# of Datacenters	Mitigation Tier**	Overage Rate**		Filtered DDoS Event Cap**
1	50 Gbps	\$15 / Mbps		\$35,000
Monthly Filtered DDoS Event Limit	Floating Filtered DDoS Event Limit	Additional Filtered DDoS Event Fee**	# of GRE Tunnels supported	# of VIPs supported
N/A	N/A	N/A	4	10


\* If this is N/A, any references herein to the terms that apply to Verisign providing monitoring, detection and/or similar services in this Service Order Form do not apply to Customer and shall not create any obligations on Verisign to monitor Customer's Internet Traffic to detect potential DDoS Events.

\*\* If applicable, Additional Filtered DDoS Event Fee, Overage Rate, Mitigation Tier, and Filtered DDoS Event Cap are per Filtered DDoS Event as defined herein.

VERISIGN SARL

CUSTOMER

By:   
 Name: Josephine Cavedon  
 Title: Authorized Signatory  
 Date: 17-MAR-2014

By:   
 Name: GABRIEL LAN  
 Title: DIRECTOR, IT SECURITY & COMPLIANCE  
 Date: MAR 14/14





### TERMS AND CONDITIONS

1. Fees. Customer shall pay the fees set forth in Table 1 above and shall pay all invoiced amounts in accordance with Section 2(c) of the MSA (except as otherwise noted below). Notwithstanding anything in the Agreement to the contrary, in the event that Verisign determines that Customer will not be granted net credit terms at the outset and/or Customer exceeds its credit limit during the Term, then Verisign may, in its sole discretion require (i) that payment be due upon receipt of invoice; and/or (ii) prepayment. In such cases, Verisign will send written notice to Customer and such written notice shall be incorporated by reference into this Service Order Form.

1.1 Non-Recurring Fee. The Non-Recurring Fees for the Verisign DDoS Protection Service are one-time fees, such as a Customer Set Up Fee, which are invoiced following the Service Order Form Effective Date.

1.2 Recurring Fees. Following the Service Order Form Effective Date, Verisign will invoice Customer in advance for the Recurring Fees in accordance with the billing frequency (e.g., monthly, quarterly, annually) described in the column entitled "SKU# and Description" in Table 1 above.

2. Suspension for Nonpayment; Fees for Collection Efforts. Notwithstanding anything in the Agreement to the contrary, Customer acknowledges and agrees that Verisign may suspend performance of and/or access to any or all of the Verisign DDoS Protection Service, discontinue the provision of any or all of the Verisign DDoS Protection Service, or terminate this Service Order Form in its entirety for non-payment or repeated late payment of the fees upon providing twenty four (24) hours prior written notice (which may be via email) of its intent to do so. In addition to any other remedies Verisign may have under the Agreement, Customer will be responsible for, and reimburse Verisign for, any and all costs, expenses and fees associated with efforts to collect unpaid amounts including, but not limited to, third party collection agency fees and reasonable attorneys' fees.

3. Term. Upon expiration of the Initial Term, this Service Order Form shall automatically terminate unless otherwise agreed to in writing by the Parties.

\*\*\*\*\*

### Exhibit A -- Service Description for Verisign DDoS Protection Services

#### 1. Definitions.

1.1 "Additional Filtered DDoS Event Fee" shall be the fee per Filtered DDoS Event in excess of the Monthly Filtered DDoS Event Limit and/or Floating Filtered DDoS Event Limit (if applicable).

1.2 "Datacenter" means a facility used to house Customer computer and/or network systems and when configured as a site where Verisign will return Customer's Internet Traffic as described herein (including, but not limited to, in Section 2.2.3) via (i) up to four (4) GRE Tunnels (as defined herein) and/or (ii) VIPs (as defined herein).

1.3 "Emergency Maintenance" means downtime outside of Regularly Scheduled Maintenance due to the application of urgent patches, fixes or other urgent maintenance. In the event of an Emergency Maintenance, Verisign will use reasonable efforts to notify Customer (email being sufficient) as soon as it is possible.

1.4 "Filtered DDoS Event" occurs when Customer's Internet Traffic has been redirected to the Verisign DDoS Protection site and continues until the earlier of (i) the time in which Customer is returned to normal operations (i.e., Customer's Internet Traffic is no longer being redirected to the Verisign DDoS Protection site); or (ii) expiration of twenty-four (24) hours regardless of the number of DDoS Events the Customer experiences during this timeframe. If the Filtered DDoS Event continues beyond twenty-four (24) hours, it will be considered a new Filtered DDoS Event.

1.5 "Filtered DDoS Event Cap" is the maximum amount that Customer will pay Verisign when a Filtered DDoS Event exceeds the Mitigation Tier regardless of duration.



VERISIGN

1.6 "Floating Filtered DDoS Event Limit" shall mean a Filtered DDoS Event that can be used at any time during the Initial Term and during each subsequent twelve (12) month Renewal Term thereafter (with no carryover) consistent with the terms and conditions contained in the Agreement. As necessary, Floating Filtered DDoS Events will be automatically deducted from the Customer's available Floating Filtered DDoS Event Limit pool upon exhaustion of the Monthly Filtered DDoS Event Limit. For the avoidance of doubt, any Renewal Term less than twelve (12) months shall have a Floating Filtered DDoS Event Limit of none (or N/A) regardless of the amount entered into Table 1 above.

1.7 "GRE Tunnel" shall mean a tunneling protocol used to encapsulate point-to-point links between Verisign's mitigation centers and Customer's router that may be used to return Customer's Internet Traffic.

1.8 "Mitigation Tier" means the maximum amount of Customer's Internet Traffic in Gbps for all Datacenters (or on a cumulative basis if Datacenters are concurrently affected at the same time) for each Filtered DDoS Event.

1.9 "Monitored Entity" shall mean one or more IP addresses designated as a sub-set of a Customer's Internet Traffic for dynamic profiling.

1.10 "Monthly Fees" shall mean the (i) Recurring Fees in the case of a monthly billing frequency; (ii) Recurring Fees divided by three (3) in the case of a quarterly billing frequency; and (iii) Recurring Fees divided by twelve (12) in the case of annual billing frequency.

1.11 "Monthly Filtered DDoS Event Limit" shall mean the maximum number of Filtered DDoS Events per month.

1.12 "Overage Rate" means the rate per Mbps (or Gbps) which shall apply when a Filtered DDoS Event exceeds the Mitigation Tier regardless of duration.

1.13 "Peak" means the maximum number in Gbps (rounded to the nearest whole Gbps) which Customer's Internet Traffic reached at any given time during a Filtered DDoS Event. For example, if the Customer's Internet Traffic reached the following Gbps, it would be rounded accordingly: 95.4 Gbps (rounded down to 95 Gbps) and 95.5 Gbps (rounded up to 96 Gbps). For the avoidance of doubt, in the event more than one Datacenter is affected by a Filtered DDoS Event at the same time, the Peak shall be the cumulative total of Customer's Internet Traffic reached at any given time during such Filtered DDoS Event over all the concurrently affected Datacenters.

1.14 "Regularly Scheduled Maintenance" means any maintenance performed during a maintenance window. Verisign will notify Customer (email being sufficient) at least forty eight (48) hours in advance of any Regularly Scheduled Maintenance.

1.15 "VIP" shall mean a virtual IP address that Verisign DDoS Protection Service designates to Customer for the redirection of Customer's Internet Traffic.

## 2. Service Description.

### 2.1 Verisign DDoS Protection Service.

2.1.1 Subject to the terms and conditions of this Service Order, Verisign will provide Customer with a DDoS Event (as defined below) mitigation service which monitors Customer's network in order to detect and, if needed, filters malicious traffic aimed at disrupting or disabling Customer's Internet-based services (the "Verisign DDoS Protection Service"). A distributed denial of service event ("DDoS Event") is an attempt from external sources to make Customer's Internet-based services unavailable to its intended users as measured and determined by Verisign.

2.1.2 With respect to mitigation, a portion or all of Customer's Internet Traffic (as designated in the Customer Information Document which is defined below) is redirected to the Verisign DDoS Protection sites during a DDoS Event. The term "Internet Traffic" shall include, but not be limited to, all Web, VPN, electronic mail, file transfer or



other data that traverses through any packet network regardless of whether the foregoing is filtered by Verisign under a Filtered DDoS Event or reported to Customer in the Customer Portal (as defined herein).

2.1.3 Under this Service Order Form, Customer hereby acknowledges and agrees that Customer is responsible for the monitoring requirements contained herein and that Verisign will (i) provide only mitigation services to Customer; (ii) not provide any monitoring services to Customer; and (iii) have no liability for failure to monitor and/or detect a potential DDoS Event. Customer further acknowledges and understands that Customer must notify Verisign if Customer is experiencing or believes it is experiencing a DDoS Event.

## 2.2 Service Components.

### 2.2.1 Customer Set-up.

(a) Assessment Call. During the kick-off meeting (the "Assessment Call"), Verisign and Customer will address the following topics: (i) introduce key people at Customer and Verisign; (ii) exchange contact information; (iii) review and collect information for the Customer Information Document which will be provided to, and must be completed by, Customer as soon as possible after Customer executes the Agreement (the "Customer Information Document"); and (iv) discuss the changes to be implemented by Customer. Customer hereby acknowledges and agrees that final configurations depend upon completion of the Customer Information Document.

(b) Monitoring and Mitigation Set-up. Once Verisign determines that Customer has completed the Customer Information Document and implemented its changes (including, but not limited to, its configuration file(s)), Verisign will perform configurations in order to detect, monitor and mitigate as more fully described in Sections 2.2.2-.3 below.

(c) Account Set-up. Verisign will set up an account for Customer in the Customer Portal (as defined below) which includes (i) inserting Customer's name and contact information, relevant information from the Customer Information Document and the final configuration file(s) to be implemented by Customer; and (ii) providing Customer with a username and password for the Customer Portal.

(d) Customer Training. Verisign will provide Customer with one (1) basic training session on the Customer Portal.

(e) Scheduling of Operational Testing. Verisign and Customer will schedule a time and date to conduct operational testing of the Verisign DDoS Protection Service during Customer Set-up.

### 2.2.2 Detection for Monitoring.

(a) Monitoring. Customer's Internet Traffic is monitored by Verisign on a 24 x 7 basis. In order to detect unusual Internet Traffic patterns, Verisign analyzes samples of Customer's traffic flow data. This data is then incorporated into Verisign's correlation engine for threat detection, alerts and reporting. Except as otherwise provided for in the Agreement, Verisign will only use such data in order to perform the Verisign DDoS Protection Service.

(b) Analysis. Potential DDoS Events will be identified by either Verisign (if applicable) and/or Customer and flagged for additional analysis.

(i) Signature Analysis. Signature analysis, or misuse detection, looks for predefined deviations that are signs of a DDoS Event.

(ii) Dynamic Profiling. Verisign uses the traffic flow analyses to establish a dynamic profile of Customer's Internet Traffic.

(c) Notice.



(i) If Customer selects Mitigation Only, Customer will notify Verisign (via telephone with a confirmation by email) in accordance with the escalation plan in the Customer Information Document ("Escalation Plan") in the event that Customer is experiencing a DDoS Event.

(ii) If Customer selects Monitoring Only or Monitoring Plus Mitigation, Verisign will notify Customer in accordance with the Escalation Plan completed by Customer if Customer's Internet Traffic (1) exhibits predefined deviations that are signs of a DDoS Event; or (2) deviates from Customer's profile and that deviation exceeds pre-defined thresholds.

**2.2.3 Mitigation.** After notification under Section 2.2.2(c), Verisign will work with Customer to mitigate the attack by providing a recommended course of action. Verisign will provide such recommendation in accordance with the Service Level Agreement set forth in Section 9 herein. In the event that redirecting the Customer's Internet Traffic is the recommended course of action, the following steps will apply:

(a) **Off-ramping Traffic.** Customer's Internet Traffic destined for Customer's Internet-based service must be redirected to the Verisign DDoS Protection sites before reaching Customer's network which can be accomplished through either a BGP swing or a DNS based swing.

(b) **Filtering.** Verisign will apply layered filters to the Internet Traffic redirected to the Verisign DDoS Protection sites which progressively block traffic aimed at disrupting or disabling Customer's Internet-based services. Customer acknowledges and agrees that Verisign will only filter the amount of Customer's Internet Traffic that is necessary to make Customer's Internet-based services available to its end user customers.

(c) **On-ramping Traffic.** After the filtering process described above is performed, Customer's Internet Traffic is redirected from the Verisign DDoS Protection sites back to Customer's network.

(d) **Normal Operations.** When Verisign has determined that the DDoS Event has abated, Verisign will coordinate with Customer in order to return Customer to its normal operations. In the event that Customer does not discontinue redirecting its Internet Traffic to the Verisign DDoS Protection sites within twelve (12) hours of Verisign's determination that the DDoS Event has abated, Verisign will invoice Customer, and Customer shall pay, a fee in the amount of \$10,000 per day for each day (or any portion thereof) not to be pro-rated after the expiration of such twelve (12) hours until Customer's Internet Traffic is no longer redirected to the Verisign DDoS Protection sites. Verisign shall invoice Customer for the fees described herein monthly in arrears. Customer shall pay the invoiced amounts in accordance with Section 2(c) of the MSA.

**2.2.4 Customer Portal.** Verisign will provide Customer with access to a web-based portal (the "Customer Portal") in order to view its traffic, reports, alerts and account information. Verisign will conduct Regularly Scheduled Maintenance on the Customer Portal from time to time. Verisign will notify Customer at least forty eight (48) hours in advance of any Regularly Scheduled Maintenance. In the event of downtime of the Customer Portal outside of Regularly Scheduled Maintenance hours due to Emergency Maintenance, Verisign will use reasonable efforts to notify Customer as soon as it is possible.

### **2.3 Conditions and Limitations.**

2.3.1 If Verisign determines, in its sole discretion, using commercially reasonable standards, that Customer's DDoS Event (a) cannot be mitigated by the Verisign DDoS Protection Service; (b) is impacting the overall stability of Verisign; (c) is impacting Verisign's ability to operate the Verisign DDoS Protection Service in a cost-effective manner; or (d) exceeds the Mitigation Tier by at least 3 Gbps (collectively (a), (b), (c), and (d) referred to herein as "Infrastructure Limitations"), Verisign may immediately choose (i) not to accept all or part of Customer's Internet Traffic; or (ii) drop all or a part of Customer's Internet Traffic from the Verisign DDoS Protection sites. In the event Verisign exercises its rights due to Infrastructure Limitations, and provides Customer written notice of the same, either party may terminate this Service Order Form immediately and without penalty for up to thirty (30) days from the date of Verisign's written notice; provided, however, Customer shall remain liable to Verisign for all unpaid fees for the Verisign DDoS Protection Services provided up to the date of termination of the Service Order Form.



2.3.2 Customer represents and warrants that (i) it has obtained any necessary consents and permissions to provide Customer and/or third party information (including personal data) to Verisign; (ii) the use of the Verisign DDoS Protection Service is for its own internal use and not for resale by Customer; and (iii) it is not engaged in any illegal activities and that it will comply with all applicable rules, regulations, laws and reasonable testing procedures and/or usage guidelines which may be provided or posted by Verisign in writing from time to time.

2.3.3 Customer agrees and acknowledges that Verisign may be required to disclose information or data about DDoS Events to law enforcement officials and/or National Computer Response Teams ("CERTs"), and that Verisign will not be liable for such required disclosure. If such information or data about a DDoS Event relates to Customer, Verisign will (i) to the extent permitted by law provide Customer with notice of such required disclosure; and (ii) reasonably cooperate with Customer's efforts to secure a protective order or other legal remedy to prevent the disclosure.

2.3.4 Customer agrees and acknowledges that Verisign may publish aggregate data; *provided, however*, that such publications will not identify Customer.

2.3.5 Customer hereby acknowledges that the Verisign DDoS Protection Service is subject to certain technical limitations and is designed to defend against known forms of DDoS Events, and that Customer has had the opportunity to discuss these limitations with Verisign. In addition, Customer acknowledges that the Verisign DDoS Protection Services utilize a shared platform. As a result, the Verisign DDoS Protection Service may not detect and mitigate all DDoS Events and, although Verisign has and will use commercially reasonable efforts to operate the Verisign DDoS Protection Service in order to detect and mitigate both known and unknown DDoS Events, Verisign cannot guarantee that all DDoS Events will be detected and mitigated. In addition, the Verisign DDoS Protection Service is not designed to address failures by upstream providers to transmit Internet Traffic.

2.3.6 Customer hereby acknowledges that Verisign's Acceptable Use Policy (the "AUP") set forth in Section 10 herein forms a part of the terms and conditions of the Agreement. Customer agrees to comply with the AUP.

2.4 Security Phrase. Verisign will provide Customer with a security phrase which Customer must provide to Verisign via telephone during the notification process described herein or in the event Customer contacts Verisign with respect to the Verisign DDoS Protection Service.

2.5 Customer Support. Verisign will provide telephone and e-mail support to Customer on a 24x7 basis. Standard support will include the following: (i) assistance with configuration; (ii) questions/troubleshooting related to the Verisign DDoS Protection Service; (iii) event notification; (iv) event mitigation; and (v) account change support.

3. Customer Obligations. As a condition to Verisign providing Customer with the Verisign DDoS Protection Service set forth above, Customer acknowledges and agrees that it is solely responsible for the following:

3.1 Customer will complete the Customer Information Document. Customer represents and warrants that the information in the Customer Information Document is accurate, reliable and complete, and that Customer will update the Customer Information Document as needed on a timely basis. If Customer does not have the necessary hardware in order for Verisign to deliver the Verisign DDoS Protection Service, the Verisign DDoS Protection Service will terminate immediately.

3.2 Customer will cooperate with Verisign to (i) determine initial minimum thresholds for Customer's Internet Traffic; and (ii) adjust minimum thresholds during the Term on an as needed basis.

3.3 Customer will make changes or direct its hosting and/or service providers to make changes to existing network equipment and/or infrastructure in order to enable Verisign to provide the Verisign DDoS Protection Service. Customer will be responsible for obtaining all necessary authorizations and permissions to effect such changes, and Customer will also be responsible for all fees or charges involved in getting Customer's Internet Traffic to the Verisign DDoS Protection sites including, but not limited to, switch and transport charges, if any, for Off-ramping and On-ramping Internet Traffic as contemplated in Section 2.2.3 above.



3.4 Customer will provide Verisign with points-of-contact to assist Verisign with Customer Set-up and deployment of, as well as on-going support for, the Verisign DDoS Protection Service. Customer points-of-contact will be available and will respond to Verisign in accordance with the Escalation Plan.

3.5 Customer will support and assist Verisign with operational testing of the Verisign DDoS Protection Service during Customer Set-up and periodically throughout the Term.

3.6 Customer will take all reasonable steps to protect against unauthorized access to, use, and disclosure of (i) its username and password provided by Verisign in order for Customer to access the Customer Portal; and (ii) security phrase provided by Verisign.

4. **Fees.** Customer shall pay the fees set forth in Table 1 of the Service Order Form and such other fees described below for the Verisign DDoS Protection Service. Customer shall pay all invoices in accordance with Section 2(c) of the MSA.

4.1 Intentionally Omitted

4.2 Recurring Fees.

4.2.1 Intentionally Omitted.

4.2.2 Mitigation Only. The Recurring Fees for Mitigation Only include mitigation for Filtered DDoS Events up to the applicable Mitigation Tier.

4.2.3 Monitoring Plus Mitigation. The Recurring Fees for Monitoring Plus Mitigation include: (i) Recurring Fees for monitoring; and (ii) Recurring Fees for mitigation, which includes mitigation for Filtered DDoS Events up to the applicable Mitigation Tier.

4.3 Additional Fees. Additional fees ("Additional Fees") may apply for the Verisign DDoS Protection Service.

4.3.1 Intentionally Omitted.

4.3.2 Mitigation Only or Monitoring Plus Mitigation. With respect to Mitigation Only or Monitoring Plus Mitigation, Additional Fees will apply for each Filtered DDoS Event which exceeds the Mitigation Tier regardless of duration; provided that such Additional Fees shall not exceed the Filtered DDoS Event Cap. The Additional Fees are determined by multiplying Overage Rate by (Peak minus Mitigation Tier) not to exceed the Filtered DDoS Event Cap.

**Customer Examples:** Customer selects Mitigation Only or Monitoring Plus Mitigation which has a Mitigation Tier of 50 Gbps, an Overage Rate of \$15/Mbps (\$15,000/Gbps) and a Filtered DDoS Event Cap of \$100,000. These examples are for illustrative purposes only with relation to the Additional Fees and shall in no way limit either party's other rights and remedies contained in this Service Order Form (including, but not limited to, those termination rights contained in Section 2.3.1).

(a) **Example 1 (Filtered DDoS Event Cap Example):** Customer experiences a Filtered DDoS Event in excess of the Mitigation Tier that lasts for twenty (20) hours. The Peak of the Filtered DDoS Event was 60 Gbps. Verisign shall invoice Customer for an Additional Fee equaling \$100,000. The calculation for the Additional Fee of \$100,000 is determined as follows: (60 Gbps minus 50 Gbps) x \$15,000 (Overage Rate) = \$150,000 which exceeds the Filtered DDoS Event Cap of \$100,000 by \$50,000, as such the Additional Fee that Verisign will invoice the Customer for is \$100,000.

(b) **Example 2 (Concurrent Cumulative Example):** Customer experiences a Filtered DDoS Event with either multiple DDoS Events or that spans across multiple Datacenters at the same time in excess of the Mitigation



Tier that lasts for twenty (20) hours. The Customer's Internet Traffic during the Filtered DDoS Event reaches a concurrent cumulative Peak of 51 Gbps. Verisign shall have the right to invoice Customer for an Additional Fee equaling \$15,000. The calculation for the Additional Fee of \$15,000 is as follows: (51 Gbps minus 50 Gbps) x \$15,000 (Overage Rate) = \$15,000.

(c) **Example 3 (Multi-DDoS Event Example):** Customer experiences a Filtered DDoS Event in excess of the Mitigation Tier that lasts for twenty-eight (28) hours. Because the total time of this Filtered DDoS Event exceeds twenty-four (24) hours, it is treated as two separate Filtered DDoS Events. The Peak of the Filtered DDoS Event 1 was 60 Gbps (during hours 0-24) and the Peak of the Filtered DDoS Event 2 was 55 Gbps (during hours 24:00:01-28:00:00). Verisign shall invoice Customer for an Additional Fee equaling \$175,000. The calculation for the Additional Fee of \$175,000 is determined as follows: Filtered DDoS Event 1 [(60 Gbps minus 50 Gbps) x \$15,000 (Overage Rate) = \$150,000 which exceeds the Filtered DDoS Event Cap of \$100,000 by \$50,000]; Filtered DDoS Event 2 [(55 Gbps minus 50 Gbps) \* \$15,000 (Overage Rate) = \$75,000]. Verisign will invoice Customer an Additional Fee of \$175,000 which equates to the sum of the Filtered DDoS Event Cap 1 (\$100,000) and the Filtered DDoS Event 2 Additional Fees of \$75,000.

**4.3.3 Invoicing.** Verisign shall invoice Customer for any Additional Fees during the month following the month in which Customer experienced the Filtered DDoS Event.

**4.3.4 Notwithstanding anything in the Agreement for the Verisign DDoS Protection Service to the contrary,** Customer may choose to discontinue redirecting Customer's Internet Traffic to the Verisign DDoS Protection sites at any time during a Filtered DDoS Event in accordance with the Escalation Plan. In such cases, Verisign will have no liability and Customer will be solely responsible for mitigating the Filtered DDoS Event once the filtering process is turned off and Customer's Internet Traffic is no longer being redirected to the Verisign DDoS Protection sites; provided, however, Customer shall be responsible for all fees incurred while Customer's Internet Traffic was directed to the Verisign DDoS Protection sites and/or the Filtered DDoS Event was being managed by Verisign.

**4.3.5 Customer hereby acknowledges and understands that net credit terms may not be granted to Customer for payment of Additional Fees if Customer exceeds its credit limit with Verisign.** In such cases, payment will be due upon receipt of the invoice.

**5. License and Use of Data.** During the Term, Verisign grants to Customer, and Customer accepts, a limited, non-exclusive, non-transferable, non-sublicensable license to access the Customer Portal solely for the purposes of viewing and managing Customer's account and the data therein and solely in accordance with any applicable instructions or documentation provided by Verisign. Customer is expressly prohibited from permitting either direct or indirect use of the Customer Portal by any third party. Customer shall not modify, disassemble, decompile, reverse engineer, create derivative works of, or make any other attempt to discover or obtain the source code for any of the software or systems which deliver the Verisign DDoS Protection Service. Verisign retains all Intellectual Property Rights (as defined in the MSA), title to and interest in all other information, data, content, software, ideas, concepts, techniques, processes, configurations or other intellectual property embodied in or practiced in connection with the Verisign DDoS Protection Service (including the Customer Portal). All such intellectual property of Verisign is deemed Confidential Information subject to Section 5 of the MSA. Verisign may request Customer testimonials and/or develop documentation relating to Customer's experience for use in case studies and marketing collateral; *provided, however,* that Verisign will not use Customer's name without Customer's prior written consent.

**6. Termination.** Notwithstanding anything in the Agreement to the contrary and in addition to Verisign's rights set forth in the Agreement, Verisign may terminate this Service Order Form immediately upon notice to Customer (i) in the event that Verisign determines, in its sole discretion, that Customer has breached Section 2.3.2 herein; (ii) in the event that Verisign determines, in its sole discretion, that it cannot increase the credit limit or grant net payment terms to Customer at any time during the Term; or (iii) for convenience within ten (10) business days of the Effective Date.

**7. Customer's Additional Indemnification Obligations.** In addition to Customer's indemnification obligations set forth in the MSA, Customer shall indemnify, defend and hold harmless Verisign and its officers, directors, agents, employees, contractors, successors and assigns (the "Verisign Parties") from and against any and all third party



claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative), judgments, and costs and expenses (including reasonable attorneys' fees and expenses) incurred by any Verisign Party arising out of, or directly or indirectly relating to (a) Customer's breach or alleged breach of the AUP or action taken, or in action, by Verisign in connection with the AUP (including, but not limited to, in relation to any violation of the AUP); (b) Customer's breach or alleged breach of Section 2.3.2; (c) Customer's use of the Verisign DDoS Protection Service which is not in accordance with this Service Order; or (d) use or failure of Customer's services. This Section shall survive termination or expiration of this Service Order Form.

**8. LIMITATION OF LIABILITY.** NOTWITHSTANDING ANYTHING TO THE CONTRARY, (A) CUSTOMER'S INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 7 ABOVE SHALL NOT BE SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN SECTION 8 OF THE MSA; AND (B) VERISIGN SHALL HAVE NO LIABILITY (I) TO THE EXTENT THAT CUSTOMER DELAYS IN REDIRECTING ITS INTERNET TRAFFIC OR IN THE EVENT THAT CUSTOMER DOES NOT REDIRECT ITS INTERNET TRAFFIC OR DISCONTINUES REDIRECTING ITS INTERNET TRAFFIC DURING A FILTERED DDOS EVENT; AND (II) WITH RESPECT TO THE AUP OR ANY ACTION TAKEN, OR INACTION, BY VERISIGN IN CONNECTION WITH THE AUP (INCLUDING, BUT NOT LIMITED TO, IN RELATION TO ANY VIOLATION OF THE AUP). IN ADDITION TO SECTION 6(F) OF THE MSA, THE VERISIGN DDOS PROTECTION SERVICE IS PROVIDED "AS IS", "AS AVAILABLE" AND WITHOUT ANY WARRANTY WHATSOEVER.

#### **9. Service Level Agreement**

##### **9.1 Service Level Descriptions.**

**9.1.1 Monitoring Set-up.** Verisign will complete the monitoring portion of the Customer Set-up as determined by Verisign ("Monitoring Set-up") in accordance with the Service Level set forth below. Monitoring Set-up will commence upon execution of this Service Order by both parties, completion of the Customer Information Document by Customer, and verification by Verisign that Customer has made all required configuration changes and completed all required obligations described in Section 3.

**9.1.2 Event Mitigation Recommendation.** Verisign will provide Customer with a recommended course of action in accordance with the Service Level described below in Section 9.2. The time period described below will commence from the time Verisign receives an alert from the monitoring platform and Verisign determines that Customer is under a potential DDoS Event.

**9.1.3 Mitigation.** Verisign will make the Verisign DDoS Protection Service for the purpose of mitigation available to Customer in accordance with the Service Level described below once Customer's Internet Traffic is redirected to the Verisign DDoS Protection Services for mitigation in response to a confirmed DDoS Event until Customer's Internet Traffic is returned to normal operations in accordance with Section 2.2.3. For purposes of the Service Level for mitigation, a "Mitigation Service Outage" means that the Verisign DDoS Protection Service, for the purpose of mitigation, was unavailable to Customer (i.e., the mitigation platform did not respond to DNS or HTTP queries) for more than sixty (60) consecutive seconds. The duration of the Mitigation Service Outage shall be determined by using information collected from Verisign's trouble tickets and/or data collected on Verisign's mitigation platform.

**9.1.4 Mitigation Start.** Provided that Customer has been fully provisioned, in the event that Customer and Verisign agree to redirect Customer's Internet Traffic to the Verisign DDoS Protection Service for the purpose of mitigation, Verisign will (i) in the case of a BGP swing, initiate redirecting Customer's Internet Traffic within fifteen (15) minutes of reaching such agreement; or (ii) in the case of a DNS-based redirect, confirm to Customer that redirection of Customer's Internet Traffic can begin within fifteen (15) minutes of reaching such agreement.

##### **9.2 Service Level Credits.**

Description	Service Level	Credit
-------------	---------------	--------





Monitoring Set-up	Greater of 14 calendar days or # of monitored routers * 2 Days	50% of Customer Set-up Fee
Event Mitigation Recommendation	15 minutes or less	One day share of Monthly Fee
Mitigation	99.999% availability	Mitigation Service Outage of 5 consecutive minutes to 4 consecutive hours = 5 days share of the Monthly Fee Mitigation Service Outage of more than 4 consecutive hours = 50% of Monthly Fee
Mitigation Start	15 minutes or less	One day share of Monthly Fee

9.3 **Reporting.** In order to receive a Service Level Credit, (i) Customer must make a claim in writing (which may be in the form of an email) to Verisign's Customer Service within fourteen (14) days of the date on which it believes the particular Service Level was not met; and (ii) Verisign must confirm that the particular Service Level was not met. Verisign's records will control for the purposes of (a) confirming whether a Service Level was not met; and (b) in the case of mitigation, determining the Mitigation Outage Time in the event that Verisign does confirm that this Service Level was not met. Verisign will make all credit determinations in its reasonable discretion and will notify Customer of its decision; *provided, however*, that Verisign shall have no obligation to issue Service Level Credits in excess of the prior month's total charges payable by Customer to Verisign under this Service Order. If any request for a Service Level Credit is rejected, the notification will contain the reasons for such rejection.

9.4 **Remedy.** Notwithstanding anything to the contrary in the Agreement, the foregoing Service Level Credits are Customer's sole and exclusive remedy for Verisign's failure to meet any Service Level. Customer shall not be entitled to any Service Level Credits (i) for Verisign's failure to meet a Service Level that are caused by or result from Customer's failure to perform its responsibilities hereunder; (ii) unless Customer has paid Verisign all amounts due and is otherwise in full compliance with the Agreement; or (iii) during Emergency Maintenance or Regularly Scheduled Maintenance.

10. **Acceptable Use Policy.** This Section 10 set forth Verisign's Acceptable Use Policy (the "AUP") which provides Customer with a set of principles, rules and guidelines for the use of information obtained by Customer from the Internet. Verisign may, in its sole discretion, change or update this AUP at any time by providing notice to Customer via email. The updated AUP shall be deemed to replace the prior version fifteen (15) calendar days after Customer's receipt of such email.

#### 10.1 **Customer's Responsibilities.**

10.1.1 Customer agrees to use the Verisign DDoS Protection Service in compliance with all applicable local, state federal or international laws, and any reasonable testing procedures and/or usage guidelines which may be provided or posted by Verisign in writing from time to time. Customer understands that Verisign may suspend Customer's access to the Verisign DDoS Protection Service if Customer fails to comply with such guidelines.

10.1.2 Customer agrees to comply fully with all applicable laws concerning the privacy of on-line communications and the provision of Internet services. Any failure by Customer to comply with those laws will constitute a breach of this AUP.

10.1.3 Customer acknowledges that information reaching the facilities of Verisign or its vendors may have originated from a customer of Customer, or from another third party. As a result, Customer agrees that Verisign or its vendors, as the case may be, may request Customer to take action against its customers directly.

10.1.4 Customer agrees to cooperate with Verisign and/or its vendors in any corrective or preventive action that either Verisign or its vendors deem necessary. Failure to cooperate with such corrective or preventive measures is a breach of this AUP.

10.2 **Prohibited Activities.** Customer shall not undertake, or attempt to undertake, any of the prohibited activities listed below. Customer further agrees that it shall take reasonable steps to ensure that any other person or party



whom Customer permits to use the Verisign DDoS Protection Service, does not undertake or attempts to undertake any of the prohibited activities listed below.

**10.2.1 Spamming.** This means sending unsolicited bulk and/or commercial electronic messages over the Internet, providing a capability on websites (which may include, but not be limited to, parked pages and online cards) hosted by Customer that permits third parties to spam from the server of Customer or its vendor or maintaining an open SMTP relay.

**10.2.2 Intellectual Property and Privacy Violations.** This means engaging in any activity that (i) infringes or misappropriates third party intellectual property rights (including, but not limited to, copyrights, trademarks, service marks, trade secrets, patents and software piracy); or (ii) engaging in software piracy (i.e., installing or distributing "pirated" software precuts that are not appropriate licensed for use; or (iii) engaging in activity that violates privacy, publicity or any other personal rights of others.

**10.2.3 Obscene Speech or Materials.** This means using the network of Verisign or its vendors (as the case may be) to collect, advertise, transmit, store, post, display, upload or otherwise make available child pornography or any other obscene speech or material. Customer agrees that where required by law, Verisign may notify law enforcement agencies when it becomes aware of the presence of child pornography on or being transmitted through the network of Verisign and/or take any other action permitted by the Service Order or this AUP.

**10.2.4 Forging of Headers, Return Addresses and Internet Protocol Addresses.** This means any forging, deleting or misrepresenting message headers, return addresses or Internet protocol addresses or otherwise manipulating identifiers, whether in whole or in part, in order to disguise the originator of the message.

**10.2.5 Illegal or Unauthorized Access to other Computers or Networks.** This means accessing illegally or without authorization computers, accounts, information or communication devices or resources or networks belonging to Verisign, its vendors or any other party, or attempt to penetrate security measures of another individual's system (often known as "hacking"). This also includes any activity that might be used as a precursor to an attempted system penetration.

**10.2.6 Distribution of Internet Viruses, Worms, Trojan Horses, or other Destructive Activities.** This means distributing information regarding the creation of and sending Internet viruses, worms, Trojan horses, ping, flooding, mail bombing, or denial of service attacks. This also includes any activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service or equipment.

**10.2.7 Facilitating a Violation of this AUP.** This means advertising, transmitting or otherwise making available any software, program, product or service that is designed to violate this AUP (including, but not limited to, by the provisioning of software that "harvests" electronic addresses from the Internet). It also includes the facilitation of the means to spam, initiation of ping, flooding, mail bombing, denial of service attacks and piracy of software.

**10.2.8 Other Illegal Activities.** This means engaging in any fraudulent or illegal activities or the sale of illegal or harmful goods or services, promoting or providing instructional information about illegal activities, promoting physical harm or injury against any group or individual or promoting any act of cruelty to animals. This may include, but is not limited to, providing instructions on how to assemble bombs, grenades, and other weapons. This also includes providing material support or resources (or to conceal or disguise the nature, location, source or ownership of material support or resources) to any organization(s) designated by the United States government as foreign terrorist organization pursuant to section 219 of the Immigration and Nationality Act. This also includes online gambling where the provision of such services violates applicable laws.

**10.2.9 Other Activities.** This means engaging in other activities, whether lawful or unlawful, that Verisign determines may damage the operations, reputation, goodwill, or customer relations of Verisign.



10.3 Verisign's Rights. If Verisign determines, in its sole discretion, that Customer has failed to comply with any provision of the AUP, or undertakes or attempts to undertake any of the prohibited activities described herein, Customer agrees that Verisign may immediately take corrective action which includes, but is not limited to, suspension of the Verisign DDoS Protection Service and/or termination of the Verisign DDoS Protection Service. Such corrective action is in addition to any other rights of Verisign under the Agreement, under this AUP or under law. Verisign may provide Customer with notice that Verisign intends to take action under this Section 10.3 but is not required to do so.

# EXHIBIT B

**From:** Lucian Florea <lflorea@tucows.com>  
**Sent:** Wednesday, December 18, 2013 5:43 PM  
**To:** Chase, Michael  
**Cc:** Adam Eisner  
**Subject:** RE: DDOS Attack  
**Attachments:** Tucows Mitigation Report 18Dec20131506.pdf

Hi Michael,

Sorry for my late reply, you can imagine we had a lot of "mopping" to do today. According to the report we are getting from verisign vdps ( see attachment) we have been indeed over 5Gb for about 12 hours. Currently we are still getting hit with about 4Gb/sec of attack traffic.

I would suggest to treat this particular incident separately, as per our current contract and have the proposed discussion in early January. Our security director is away on vacation until the end of the year and I need him definitively be part of this.

However, if you can send me some initial material about what you would like to propose - I can take a look and get an idea about our options going forward.....

Thanks,

--

Lucian Florea  
VP Technical Operations and Planning  
tucows.com